IN THE SPECIFICATION

Please amend the Title on page 1 as follows:

USER AUTHENTICATION SYSTEM ~~BASED ON ADDRESS, DEVICE THEREOF, AND PROGRAM~~ FOR PROVIDING ONLINE SERVICES BASED ON THE TRANSMISSION ADDRESS

Please amend the paragraph beginning at page 12, line 3, as follows:

The user identifier allocating means 130 acquires a user ID from user ID entry data which is stored in the user database 20, for example, and allocates the acquired user ID as a user identifier ID_U in response to the authentication request. Alternatively, the user identifier allocating means 130 may generate a random number in an encryption means 130a ~~140a~~ when it has acquired a user ID, add the generated random number to the acquired user ID, and a resulting (random number + user ID) information may be further encrypted with an identifier generating secret key K_{ID} of the authentication server 100 to be allocated as a user identifier ID_U. When arranged in this manner, only a person who knows the identifier generating secret key, for example the authentication server 100 is in a position to know the user ID on the basis of the user identifier ID_U, whereby the privacy protection of the user can be realized even though the user identifier ID_U is contained in a ticket to be transmitted to the application server. As a further alternative, the user identifier allocating means 130 may allocate a user identifier ID_U from the user authentication information or may choose something from random numbers, characters, a sequence number, which can be uniquely associated with the user ID by the database.

Please amend the paragraph beginning at page 18, line 7, as follows:

The ticket verifying means 320 verifies whether or not the ticket (CK1) 51 contained in the packet 52 is forged. The ticket verifying means 320 verifies the authentication information IA contained in the received ticket 51 in an authentication information verifier 320a, for example. Specifically, if authentication information IA is an authenticator(MAC: message authentication code), it verifies whether or not the ticket 51 has been forged in the authenticator verifier 320a using a shared secret key ~~K_{CSA}~~ K_{CAS} which is previously shared with the authentication server 100. In addition, the ticket verifying means 320 collates the address A_U contained in the ticket 51 against the source address A_S in the packet 52 in an address collator 320b, and if they do not coincide, the verification fails.

Please amend the paragraph beginning at page 19, line 6, as follows:

[0030] When a result of the collation of the address A_U contained in the ticket (CK1) 51 and the source address A_S of the packet 52 performed by the ticket verifying means 320 indicates a match and it is determined that the ticket has been transmitted from a user terminal having the authentic address, this ticket 51 is stored in the ticket memory means 330. However, if any one of other verifications and collations performed by the ticket verifying means 320 is unsuccessful, the ticket 51 is prevented from being stored in the ticket memory means 330 ~~320a~~. For example, outputs from the verifiers ~~detectors~~ 320a, 320c, and 320d and the collator 320b are input to a memory command unit 320g, and if any one of the inputs indicates unsuccessful, a command to store the ticket 51 is not generated.

Please amend the paragraph beginning at page 29, line 18, as follows:

The authentication means 420 performs an authentication of the user on the basis of user authentication information which is received by the user authentication information reception means 110. By way of example, the authentication means 420 verifies a matching

between the user authentication information and authentication data stored in the user database 20 in an authentication information collator ~~120a~~ 420a for purpose of user authentication. If required, the authentication server may also confirm whether or not a user terminal keeps a private key related to a key information IK. For example, the possession of a private key which forms a pair with an public key corresponding to a key information IK may be confirmed.

Please amend the paragraph beginning at page 32, line 2, as follows:

[0056] A key information generator 503a causes the public key K_{PU} of the user terminal 500 to be entered from a key storage 502b to generate key information IK. The key information generator 503a may deliver the entered public key directly as key information. A user authentication information transmitting means 220 transmits not only the user authentication information but also the key information to the authentication server 400 for purpose of an authentication request.

Please amend the paragraph beginning at page 32, line 9, as follows:

The service request means 530 comprises a session establishing means 532 and a packet cryptographic processing means 533, and is used to request a service provided by the application server 600. The session establishing means 532 generates in a session key generator 532a a secret key which is shared with the application server 600 as a session secret key K_{CUS} from a private key K_{SU} ~~K_{SS}~~ which forms a pair with an public key K_{PU} associated with the key information contained in the ticket 53 and the public key K_{PS} of the application server 600 in conformity to IKE (Internet Key Exchange).

Please amend the paragraph beginning at page 33, line 10, as follows:

An example of construction of a packet 54 generated by the packet cryptographic processing means 533 is shown in Fig. 16. As a distinction from the packet 52 shown in Fig. 6, the header 54h is added with an authentication header and a ticket 53 in a payload 54p is added with a key information. It is to be noted that a packet may be encrypted in the encryptor ~~532b~~ 533a and added with the authentication header AH.

Please amend the paragraph beginning at page 34, line 1, as follows:

The session establishing means 611 includes a ticket verifying means 620, and establishes a session with the user terminal 500. In a procedure which establishes the session, it shares a session secret key with the user terminal 500 in conformity to IKE or the like. Thus, the session establishing means 611 generates in a session key generator 611a a secret key which is shared with the user terminal 500 as a session secret key K_{CUS} by using a private key ~~K_{SA}~~ K_{SS} of the application server 600 stored in the key storage 602b and the public key K_{PU} of the user terminal 500.

Please amend the paragraph beginning at page 34, line 9, as follows:

[0060] After sharing the session secret key with the user terminal 500, the packet authentication means 612 verifies the authentication header AH which is added to the received packet 54 using the session secret key K_{CUS}. If a result of verification of the authentication header which is added to the packet 54 is correct, the packet authentication means 612 delivers the ticket (CK2) 53 in the packet 54 to the ticket verifying means 620. When the received packet 54 is encrypted by the user terminal 500, a packet decrypting means 612' indicated in parentheses is used instead of the packet authentication means 612, and the packet 54 is decrypted with the session secret key K_{CUS}. When properly decrypted or when the packet 54 has not been forged, the decrypted packet 54 is delivered to the ticket

verifying means 620. The authentication of the authentication header AH ~~plus~~ or the decrypting processing of the packet 54 is generically referred to as a packet verification, and an arrangement to perform such verification is referred to as a packet verifying means.

Please amend the paragraph beginning at page 43, line 24, as follows:

The user terminal 500, using a key information generator ~~503b'~~ 503a' (Fig. 21C) in the authentication request means 503, calculates a value r of one-way hash function h for ~~inputs~~ an input b and the authentication purpose shared secret key K_{US}, $r=h(K_{US}, b)$ as a response to b received, and generates a pair of the challenge b and the response r as key information IK={b, r}. This key information IK is transmitted to the authentication server 400. It is to be noted that as the challenge b, instead of a value which is explicitly transmitted from the authentication server 400 ~~500~~, an implicit challenge such as a time (time stamp) when the response is generated or a sequence number in the session may be used, and in this instance, the transmission and the reception of the challenge can be omitted.

Please amend the paragraph beginning at page 44, line 24, as follows:

In the application server 600, a terminal authenticator 620d (Fig. 21D) is further provided in the ticket verifying means 620 which enters key information IK={b, r}, [[to]] ~~recalculate~~ recalculates in a one-way hash calculator a hashed value $h(K_{US}, b)$ for the challenge b using the shared secret key K_{US}, and collates ~~collating~~ in a collation decision unit whether or not the hashed value coincides with the response r within the key information IK. If a result of the collation indicates a coincidence, a command is issued from the collation decision unit of the terminal authenticator 620d to the memory command unit 620c (Fig. 14) to permit a storage, whereby the ticket is stored.

Please amend the paragraph beginning at page 45, line 6, as follows:

[0082] Alternatively, the terminal authenticator 620d (Fig. 21D ~~21d~~) in the application server 600 may transmit an additional challenge b' in the process of establishing a session with the user terminal 500 to the user terminal, as indicated in broken lines in Fig. 21A, and receives a corresponding response $r'=h(K_{US}, b')$ from the user terminal 500 for confirming the authenticity of r'. (In this instance, b' may be replaced by an implicit challenge)